

Chapter 2

The Legal Environment and Its Impact on Information Technology

Summary/Objectives

The purpose of this chapter is to provide discussion on the legal environment and the IT auditor's role in assisting management and legal counsel. With services industry expanding, the importance of contract compliance and monitoring has grown proportionally, exceeding the abilities of the organization to successfully identify problems and alert management to take action before they become business disasters and end up in the courts. Recent rulings and laws have hastened organizations to examine corporation's use of electronic mail, intranets, extranets and the Internet itself. Government's concern for protection of individual rights has generated a frenzy worldwide and global positioning for information control and dissemination.

After completing this chapter, students should learn:

- The Auditor's role with regard to:
 - IT Crime Issues
 - IT Contracts
 - NetLaw
- Within the IT Crime Issues, we examine the
 - Categories of Crimes
 - Protection Against Computer Fraud
 - The U.S. Computer Fraud and Abuse Act and amendments
 - U.S. Legislation Providing Civil and Criminal Penalties
 - The U.S. Computer Security Act
- Exposure to the emergence of NetLaw, providing the IT Auditor of new risks businesses face as they enter competition on the Information SuperHighway:
 - Privacy Issues
 - U.S. Privacy Legislation such as the Privacy Act and the Electronic Communications Privacy Act
 - U.S. Communications Decency Act
 - Other Pending U.S. Legislation
 - Internet Governance

Tips & Tricks

Our discussion goes into the legal issues current impacting businesses worldwide, especially within the US. Educators using this text from Non-US countries may want to use this chapter to provide a base of comparison with current legal issues within their own country impacting IT business decisions. Students with a business or commerce education or experience are usually very familiar with the business law aspects.

Analogies

The easiest way to introduce the importance of this area is to ask students to conduct research about computer crimes that have been committed and the consequences to business as a result of such acts. US laws such as the HIPAA Act of 1996, the Sarbanes-Oxley Act and the Homeland Security Act have given the Auditor new support. As an IT Auditor, internal or external, what is their role should they discover computer fraud or abuse? What is the organization's legal basis for pursuing prosecution? This provides a better understanding of the importance of the audit process and the rigors of the gathering of evidence to support the audit report.

In the area of NetLaw, privacy has become a very big issue worldwide. Have the student research recent laws, which have emerged, in countries like China, Japan, Indonesia, France and Germany for privacy violations on the Internet. Certainly, Internet Governance regarding IPO naming conventions has reached the World Court.

Suggested Supplemental Material

COBIT

- See Appendix II, Publications from the AICPA, CICA, ISACA, IIA and
- US Department of Justice, US Government Accountability Office, National Institute of Standards and Technology, National Technical Information Service, Office of Technology Assessment, Privacy of Information
- See Appendix III, Guidance provided by AICPA, IIA, ISACA, CICA, IFAC and ICAA
- Handouts on IT related Laws, IT Contracting Issues and evolving NetLaw.

Examples of US Computer Laws Pertinent to IT Audit Security and Control		
US Federal Law	Effective year	Purpose
Fair Credit Reporting Act	1971	Provide protection to individual with regard to credit service bureau reporting, recent amendment places burden of proof on credit services
Privacy Act	1974	Protect individual against dissemination of Government collected information, stipulates use of information by federal agencies can only be reported in aggregate and not identify individuals
Right to Financial Privacy Act	1976	Extends elements of privacy act to financial institutions to protect individual consumer

Foreign Corrupt Practices Act	1977	Requires organizations who have foreign interests to identify such interests and system of internal controls to protect against misuse of foreign monies
Copyright Act	1976, 1980	Extends protection of Act to Computer Software. Provides guidance for source code, operating systems and databases seeking protection
Computer Fraud and Abuse Act	1984, 1986 and 1994	Felony and misdemeanor penalties and fines for Computer Fraud and Abuse
Electronic Communications Privacy Act	1986	Protects against violation of private information applicable to on-line systems
Computer Security Act	1987 and 1997	A Declaration of the Federal Government that improving the security and privacy of sensitive information in Federal computer systems is in the public interest
Federal Trade Mark Dilution Act	1997	One of the first Netlaws to deal with domain name conflicts. This has caused interest by the World Court regarding the domain naming process.
Communications Decency Act	1995	Bans the making of “indecent” or “patently offensive” material available to minors via computer networks. The Act imposes fines and imprisonment.
Health Insurance Portability and Accountability Act (HIPAA)	1996	The first-ever federal privacy standards to protect patients’ medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003.
Risk Gramm-Leach-Bliley Act	1999	The Gramm-Leach-Bliley Act signed into law on Nov. 12, 1999 requires financial institutions to Assess Risk, Manage and Control Risk, Oversee Service Providers, and Adjust security programs as needed based on changing risk. One specific provision requires the business to “Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.”
The Children's Online Privacy Protection Act	2000, 2008	The Children’s Online Privacy Protection Act was effective April 2000, and Amended in 2008 to include Title II “Protecting the Children” of the Broadband Data Improvement Act of 2008 PUBLIC LAW 110–385.” The Act specifically defines personal information for a child. This act applies to operators or owners of a commercial website or an online service directed to children under 13 that collect personal information from children or if you operate a general audience website and have actual knowledge that you are collecting personal information from children. Personal Information is defined as individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone

		number or any other information that would allow someone to identify or contact the child.
The US Patriot Act of 2001	2001	The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes. The law is intended to strengthen US measures to prevent, detect and prosecute international money laundering and financing of terrorism.
Sarbanes-Oxley Act (Public Law 107-204)	2002	This act is a major reform package mandating the most far-reaching changes Congress has imposed on the business world since the Foreign Corrupt Practices Act of 1977 and the SEC Act of the 1930s. It seeks to thwart future scandals and restore investor confidence by, among other things, creating a public-company-accounting-oversight board, revising auditor independence rules, revising corporate governance standards and significantly increasing the criminal penalties for violations of securities laws.
The Homeland Security Act	2002	The Homeland Security Act of 2002 was created to prevent terrorist attacks within the United States and reduce the vulnerability of the U.S to terrorism.

Review Questions

1. What advice does the FBI provide in protecting against computer fraud?

The Federal Bureau of Investigation's National Computer Crime Squad has the following advice to help protect against computer fraud:

1. Placing a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.
2. Turn audit trails on.
3. Consider keystroke level monitoring if adequate banner is displayed. Request trap and tracing from your local telephone company.
4. Consider installing caller identification.
5. Make backups of damaged or altered files.
6. Maintain old backups to show the status of the original.
7. Designate one person to secure potential evidence. Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.
8. Keep a record of resources used to reestablish the system and locate the perpetrator.
9. Encryption of files.
10. Encryption of transmissions.
11. Use of one-time password generators.
12. Use of secure firewalls.

2. What is software piracy? How big a problem is it? Who is the Software Publishers Association or the Business Software Alliance?

The explosion of the information Age has created many opportunities for improving business. It has also created more opportunities for criminals. Three years ago, the International Trade Commission reported that computer software piracy is a \$4 billion a year problem worldwide. Today, experts believe that software piracy costs the computer industry more than \$11 billion a year and software theft drains the U.S. economy of jobs and wages. Others estimate that there is 1 illegal copy of each computer software program for every 2 legitimate copies. Organizations such as the Business Software Alliance, Software Publishers Association, Institute of Internal Auditors and the Information Systems Audit and Control have been instrumental in raising the awareness to this type of crime.

3. What is the Computer Fraud and Abuse Act?

The CFAA was first drafted in 1984 as a response to computer crime. Government's response to network security and network related crimes was to revise the act in 1994 under the "Computer Abuse Amendments Act", to cover such crimes as trespass (unauthorized entry) into an on-line system, exceeding authorized access, and exchanging information on how to gain unauthorized access.

4. What is "reckless destructive trespass"?

Reckless Destructive Trespass—This is when there is presence of a trespass along with reckless actions (though not deliberately harmful), cause damage to a computer, computer system, network, information, data, or program, or results in denial of service, and causes at least \$1,000 total loss in the course of a year.

5. What is the Sarbanes-Oxley Act?

This act is a major reform package mandating the most far-reaching changes Congress has imposed on the business world since the Foreign Corrupt Practices Act of 1977 and the SEC Act of the 1930s. It seeks to thwart future scandals and restore investor confidence by, among other things, creating a public-company-accounting-oversight board, revising auditor independence rules, revising corporate governance standards and significantly increasing the criminal penalties for violations of securities laws.

The act discusses requirements for the Board including composition and duties. The Board must 1) register public accounting firms; 2) establish, or adopt, by rule, auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers; 3) conduct inspections of accounting firms; 4) conduct investigations and disciplinary proceedings, and impose appropriate sanctions; 5) perform such other duties or functions as necessary or appropriate; 6) enforce compliance with the Act, the rules of the Board, professional standards, and the securities laws relating to the preparation and issuance of audit reports and the obligations and liabilities of accountants with respect thereto; 7) set the budget and manage the operations of the Board and the staff of the Board.

The Sarbanes-Oxley Act of 2002 focuses on the importance of due professional care. The Sarbanes-Oxley prohibits all registered public accounting firms from providing audit clients, contemporaneously with the audit, certain non-audit services including internal audit

outsourcing, financial-information-system design and implementation services and expert services. These scope-of-service restrictions go beyond existing Security and Exchange Commission (SEC) independence regulations. All other services, including tax services, are permissible only if pre-approved by the issuer's audit committee and all such pre-approvals must be disclosed in the issuer's periodic reports to the SEC.

6. What is the Copyright Act? How is this being used in Information Technology Issues?

The 1976 Copyright Act grants civil courts the authority to grant injunctions as well as orders for impoundment and destruction of articles used in committing the fraud in disputes involving copyright infringement. This act also provides the definition of infringement for criminal prosecution. This requires that a person willfully infringe on a copyright for the purposes of personal or commercial financial gain. A party found guilty of criminal copyright infringement is subject to the forfeiture of profits from the criminal activity as well as the destruction of property used in the activity. The Copyright Act has not proven useful in court cases involving Internet fraud at this time.

7. What impact has the Federal Trademark Dilution Act had on corporation users of the Internet?

The Federal Trademark Dilution Act signed in 1996 addresses a new form of intellectual property—domain names. Under this act, domain names are now subject to trademark law. Many lawsuits have been filed in this area and to date few have gone to trial. Generally, a large corporation has sued a small business or individual and the individual cannot afford the legal costs of the battle. Out of course settlements usually result in the large corporation getting rights to the domain name they want. As you will read later in this chapter this issue has now come up at a major International Internet Conference and potential World Court involvement on the issue of Internet Governance.

The few cases that have been adjudicated have resulted in the courts finding the defendant in violation of the Federal Dilution Act. In *Intermatic Inc. v. Toepfen*, the court demanded that the domain name intermatic.com be turned over to Intermatic. There are some inconsistencies in the courts' decisions. "The federal anti-dilution of law only calls for the remedy of an order that a party cease and desist from its diluting activity. In rare cases it might allow for damages, attorney fees or the destruction of the offending goods. It does not specify that the prevailing trademark owner actually get to take possession of the diluting goods." These types of inconsistencies show that there are still many issues that need to be addressed in the field of computer legislation.

8. What is the Computer Security Act? Who does it impact? What problems has the Act encountered?

The Computer Security Act of 1987 was drafted due to congressional concerns and public awareness on computer security related issues, and because of disputes on the control of unclassified information. The general purpose of the act was a declaration from Government that improving the security and privacy of sensitive information in Federal computer systems is in the public interest.

9. What is the Homeland Security Act? Can Hackers who cause injury or death to others be prosecuted under this Act?

The Cyber Security Enhancement Act (H.R. 3482) was incorporated into the Homeland Security Act of 2002. The Act demands life sentences for those hackers that “recklessly” endanger lives. Also, the act are included provisions which seek to allow Net surveillance to gather telephone numbers, IP addresses, and URLs or e-mail information without recourse to a court, where an “immediate threat to a national security interest” is suspected. Finally, Internet Service Providers (ISPs) are required to hand users’ records over to law enforcement authorities, overturning current legislation that outlaws such behavior.

The Homeland Security Act added additional phrasing which seeks to outlaw the publication anywhere of details of such tools as PGP, which encode emails so that they cannot be read by snoops. This provision allows police to conduct Internet or telephone eavesdropping randomly with no requirement to ask a court’s permission first. As mentioned earlier, this law has a provision that calls for punishment of up to life in prison for electronic hackers who are found guilty of causing death to others through their actions. Any hackers convicted of causing injuries to others could face prison terms up to 20 years under cyber crime provisions, which are in Section 225 of the Cyber Security Enhancement Act provision of the Homeland Security Act.

10. What is the Privacy Act? What does it protect?

One of the major pieces of federal legislation to come out of the 1970s to augment the basic right to privacy that an individual is entitled to under the U.S. Constitution is the Privacy Act of 1974. The purpose of this act is to provide certain safeguards for an individual against an invasion of personal privacy.

11. What is the Electronic Communications Privacy Act, what does it protect?

The Electronic Communications Privacy Act is one of the leading legislation against violation of private information applicable to on-line systems.

12. What is the Communications Decency Act, what does it protect?

One of the most recent acts passed by Congress; the Communication Decency Act (CDA) bans the making of “indecent” or “patently offensive” material available to minors via computer networks. The Act imposes a fine of up to \$250,000 and imprisonment for up to two years. The CDA does specifically exempt from liability any person who provides access or connection to/or form a facility, system or network that is not under control of the person violating the Act. Also, the CDA specifically states that an employer shall not be held liable for the actions of an employee unless the employee’s conduct is within the scope of his or her employment.

13. What is the US plan for Securing Cyberspace?

See <http://www.whitehouse.gov/pcipb/> The National Strategy to Secure Cyberspace

14. List and explain two other bills congress has under consideration?

Can vary based on search of www.house.gov or <http://thomas.loc.gov/> or www.senate.gov key words Information Technology, Computer Crime, Computer Law, CyberLaw, Information Security, and Information Privacy.

15. Why is it important for IT Auditors to know about the legal environment of information systems?

For the IT Auditor entering the new millennium, the need to keep current of new and changes existing laws is critical. They can provide leverage in helping organization's understand the risks they face and the potential for consequences. Such consequences could even be decided at the International level as information technology issues such as Internet Governance begin to appear before the World Court. The potential for lawsuit through computer crime, invasion of privacy, copyright, patent and trademark infringement, and information technology contract nonperformance is very high. The cost is even greater in dollars and resources if the case goes to court and the company, business or industry receives negative exposure from the incident.

Exercises

1. Using an Internet web browser, perform a search on the topic "Computer crime". Examine five websites and summarize the information they provide.

Answers can vary based on searches.

2. Using an Internet web browser, perform a search on the topic "Computer Privacy". Examine five websites and summarize the information they provide.

Answers can vary based on searches.

3. Using an Internet web browser, perform a search on the topic "Computer Law". Examine five websites and summarize the information they provide.

Answers can vary based on searches.

4. Using an Internet web browser, perform a search on the topic "Computer Security Act". Examine five websites and summarize the information they provide.

Answers can vary based on searches.

5. Using the Internet web browser, look up the Software Publishers Association or Business Software Alliance.

Who are they? What help or assistance can they provide? Answers can vary based on searches.

6. Answer Case 8 in Appendix I, OHMY Corporation.

See answer in Appendix I, case 8.